BOBCOIN

(A Truly Independent Decentralized Cryptocurrency)

Chedd3r, G World, and BucketBob

Established July 3rd, 2025

Abstract. *Bobcoin (BBC) is a peer-to-peer electronic cash system that aims to eliminate the need for centralized financial intermediaries. By utilizing a robust Proof-of-Work (PoW) consensus mechanism and a double-SHA256 hashing algorithm, Bobcoin provides a secure, transparent, and immutable ledger for the digital age. This paper outlines the protocol's architecture, monetary policy, and technical specifications.*

---

1. INTRODUCTION

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Bobcoin offers an alternative: a cryptographic proof-based system that allows any two willing parties to transact directly with each other without the need for a trusted third party.

2. TRANSACTIONS AND THE LEDGER

The Bobcoin protocol manages value through a series of cryptographically signed transactions stored in a distributed ledger.

- **Transaction Structure:** Each transaction consists of inputs and outputs, ensuring that the total supply is tracked through Unspent Transaction Outputs (UTXOs).
- **Signatures:** Transactions of the "TRANSFER" type utilize Ed25519 public-key cryptography to verify the sender's identity and authority.
- **Data Integrity:** Transaction IDs are derived by taking the SHA-256 hash of the canonical JSON-serialized transaction payload.
- **Metadata:** The protocol allows for metadata to be embedded in transactions via a "memo" field, limited to 80 bytes (standard OP_RETURN size).

3. PROOF-OF-WORK CONSENSUS

To implement a distributed timestamp server on a peer-to-peer basis, Bobcoin uses a proof-of-work system similar to Adam Back's Hashcash.

- **Hashing Algorithm:** The block header is hashed using a double-SHA256 function.
- **Target and Difficulty:** For a block to be valid, its header hash must be less than or equal to a specific 256-bit target. The maximum target is 00000ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff.
- **Difficulty Adjustment:** The network adjusts the target every 120 blocks (Difficulty Adjustment Interval) to maintain a consistent block production rate based on the actual time taken to mine the previous interval.

4. NETWORK AND BLOCK PARAMETERS

The Bobcoin network is designed for efficiency and reliability with the following core parameters:

- **Target Block Time:** 5 minutes (300 seconds).
- **Maximum Block Size:** 1,000,000 bytes.
- **Transaction Limit:** A maximum of 200 transactions (plus one coinbase) per block.
- **Chain Identification:** Each network uses a unique Chain ID (e.g., bobcoin-testnet-v1) to prevent replay attacks.

5. MONETARY POLICY

Bobcoin features a strictly defined, capped supply to ensure long-term value preservation.

- **Maximum Supply:** The total supply is hard-capped at 15,000,000 BBC.
- **Initial Reward:** The initial block subsidy started at 36 BBC per block.
- **Halving Schedule:** The block reward is reduced by half every 210,240 blocks.
- **Unit of Account:** One BBC is composed of 100,000,000 atomic units, known as "BOBS".

6. SECURITY AND VALIDATION

The Bobcoin Core software performs rigorous validation on all incoming data to maintain network integrity:

- **Merkle Roots:** Each block header contains a Merkle root of all transactions, ensuring that any modification to a transaction would invalidate the entire block.
- **Coinbase Maturity:** Newly minted coins must mature for 10 blocks before they can be spent, protecting the network from instability during chain reorganizations.

- **Timestamp Protection:** Blocks must have a positive timestamp that is greater than the previous block and no further than 120 seconds into the future.

7. CONCLUSION

Bobcoin provides a framework for a truly independent decentralized currency. By combining proven cryptographic methods with a disciplined monetary policy, it offers a secure and scalable solution for peer-to-peer electronic cash.